Forensia- Tp1

Herramienta usada: CyberChef

Ejercicio - “Ocultamiento 3 - Práctica 1” (codificación) Develar el mensaje:
- 4946447b63616c656e74616e646f5f6d6f746f7265737d

IFD{calentando_motores} // Data format → From Hex

Ejercicio - “Ocultamiento 4 - Práctica 1” (criptografía) Develar el mensaje:
- VSQ{rapbqvat_rirelguvat}

IFD{encoding_everything} // Encryption/ Encoding → ROT13

Ejercicio - “Ocultamiento 9 - Práctica 1” (esteganografía)
“Te paso esta imagen para el trabajo que tenemos la semana que viene. Acordate que la clave es re simple.”:
- dino.zip

Probe en steganografhy online pero no hubo mensaje oculto ahi. (sacado de la explicacion practica)
Probe con http://futureboy.us/stegano/decinput.html tampoco me dio un mensaje. (sacado de la explicacion practica)
Use el comando steghide extract -sf dino.jpg herramienta sugerida en la explicacion practica

Use como passphrase: “re simple” “resimple” “dino” pero no funciono

```
┌──(kali㉿kali)-[~/Downloads/dino]
└─$ steghide extract -sf dino.jpg
Enter passphrase:
steghide: could not extract any data with that passphrase!

┌──(kali㉿kali)-[~/Downloads/dino]
└─$ steghide extract -sf dino.jpg
Enter passphrase:
steghide: could not extract any data with that passphrase!

┌──(kali㉿kali)-[~/Downloads/dino]
└─$
```

probe “re simple.” pero con el punto final ANDUVO!!!!!!!!!

```
┌──(kali㉿kali)-[~/Downloads/dino]
└─$ steghide extract -sf dino.jpg
Enter passphrase:
wrote extracted data to "flag.txt".

┌──(kali㉿kali)-[~/Downloads/dino]
└─$ cat flag.txt
IFD{st3g0_s3cr3t}

┌──(kali㉿kali)-[~/Downloads/dino]
└─$
```

IFD{st3g0_s3cr3t}

Ejercicio - “Ocultamiento 16 - Práctica 1” (hashing)
Él sólo habla en SHA384. Hay que decirle "puede darme la flag por favor?" Formato IFD{}

Hice un script tp1_ejer3.py para que pase el texto a SHA384 porque CyberChef no tenía esa opción de hashing.

IFD{7e100adcec2cb382a266d83d2e9a614b891f12c9ed2221ba50e6300cea56215e41affabfdab4}

```
┌──(kali㉿kali)-[~/forensia]
└─$ ls
tp1_ejer3.py

┌──(kali㉿kali)-[~/forensia]
└─$ nano --linenumbers tp1_ejer3.py

┌──(kali㉿kali)-[~/forensia]
└─$ python tp1_ejer3.py
7e100adcec2cb382a266d83d2e9a614b891f12c9ed2221ba50e6300cea56215e41affabfdab4

┌──(kali㉿kali)-[~/forensia]
└─$ cat tp1_ejer3.py
import hashlib

mensaje = "puede darme la flag por favor?"
hash_sha384 = hashlib.sha384(mensaje.encode()).hexdigest()
print(hash_sha384)
```